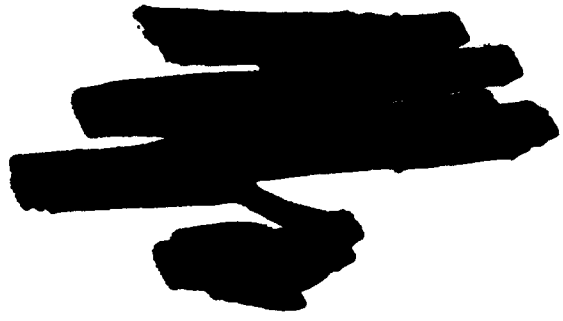
MANAGEMENT BRIEF RD-SE-94-1

INFORMATION SECURITY FOR UNMANNED SYSTEMS

John R. Coward
System Engineering and Production Directorate
Research, Development, and Engineering Center



July 1994

U.S. ARMY MISSILE COMMAND
Redstone Arsenal, Alabama 35898-5000

Approved for public release; distribution is unlimited.

DESTRUCTION NOTICE

FOR CLASSIFIED DOCUMENTS, FOLLOW THE PROCEDURES IN DoD 5200.22-M, INDUSTRIAL SECURITY MANUAL, SECTION II-19 OR DoD 5200.1-R, INFORMATION SECURITY PROGRAM REGULATION, CHAPTER IX. FOR UNCLASSIFIED, LIMITED DOCUMENTS, DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THE DOCUMENT.

DISCLAIMER

THE FINDINGS IN THIS REPORT ARE NOT TO BE CONSTRUED AS AN OFFICIAL DEPARTMENT OF THE ARMY POSITION UNLESS SO DESIGNATED BY OTHER AUTHORIZED DOCUMENTS.

TRADE NAMES

USE OF TRADE NAMES OR MANUFACTURERS IN THIS REPORT DOES NOT CONSTITUTE AN OFFICIAL ENDORSEMENT OR APPROVAL OF THE USE OF SUCH COMMERCIAL HARDWARE OR SOFTWARE.

Management Brief RD-SE-94-1

INFORMATION SECURITY FOR UNMANNED SYSTEMS

John R. Coward
System Engineering and Production Directorate

APRIL 1994

Cleared for public release; distribution is unlimited.

Research, Development, and Engineering Center
U.S. Army Missile Command
Redstone Arsenal, AL 35898

ABSTRACT

The primary mission of unmanned systems is to perform reconnaissance and gather electronic intelligence. Information gathered by these systems is most often sensitive and steps should be taken to ensure its security and integrity. This report will discuss the role of unmanned systems with resp[illegible]o intelligence gathering and give an overview of methods which can be used to ensure th[illegible]rity and integrity of the intelligence data gathered by these systems. This will include an introduction to signal scrambling, encryption techniques, and tradeoffs involved in the use of these methods of information security.

TABLE OF CONTENTS

MISSION OF UNMANNED SYSTEMS

Reconnaissance is the primary mission for unmanned systems. Unmanned systems allow collection of information without directly endangering human lives. Most unmanned systems today are man–in–the–loop systems, where an operator sends an unmanned system equipped with an array of sensors (visual, aural, infrared) into hostile territory and collects information provided by these sensors (Fig. 1). This method of intelligence collection can provide the user with information that can be critical to strategic or tactical plans. This information can be relayed back to higher headquarters where it can be integrated into the decision making process. Information collected by these unmanned systems is often very sensitive and steps should be taken to ensure the integrity of this intelligence and prevent it from falling into the hands of potential adversaries. This paper will briefly discuss the importance of information security, techniques for safeguarding information including video scrambling and data encryption, along with factors that should be considered in choosing a system for information security.

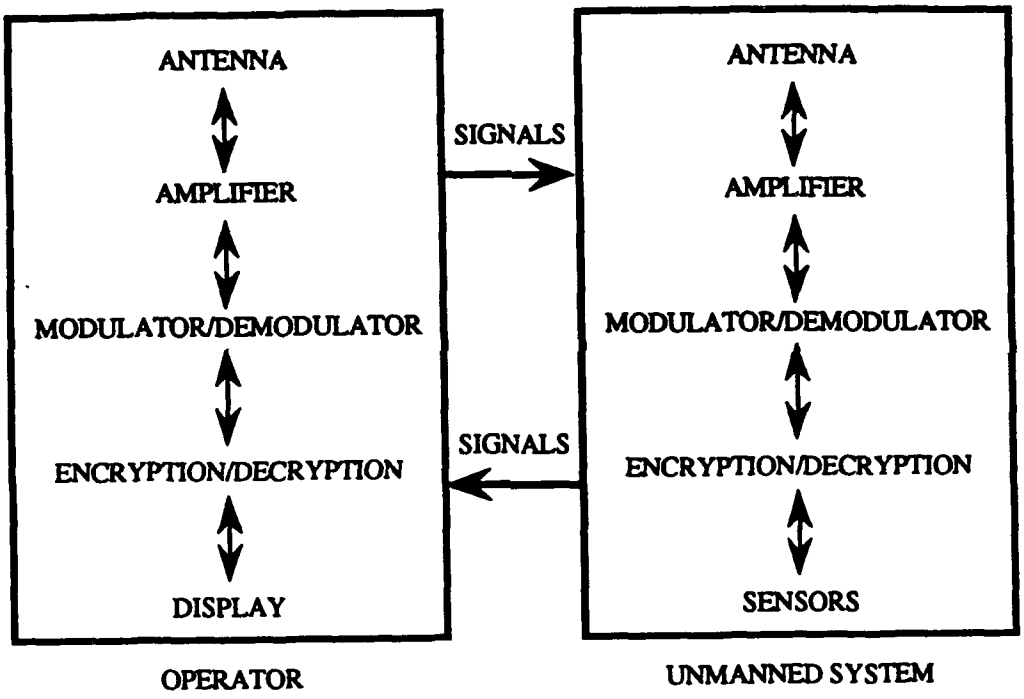


Figure 1. Generic Block Diagram of Datalink

IMPORTANCE OF INFORMATION SECURITY

The importance of information security cannot be overstated. Being able to gather and secure intelligence is critical on the modern battlefield. Technological advances in computers and communications mean that the collection and safeguarding of information is paramount to the success of any mission. The advent of the digital age means that images, communications, and intelligence are just different forms of information and the protection of this information will determine who has the advantage and who will ultimately win confrontations in the future. This extends not only to the ability to keep intelligence secret, but to ensuring the integrity of information and preventing the enemy from adulterating information which has been gathered. This threat to the integrity of information is also critical because it could lead to an unrealistic picture of actual events and corrupt the decision making process.

VIDEO SCRAMBLING

Video scrambling can be used to protect images transmitted by unmanned systems. These scrambling techniques are similar to those used by cable broadcasters to prevent interception of their signals by satellite dish owners. Scrambling most often uses signal inversion or frequency distribution schemes to secure information. There are two major types of video scrambling: signal reformatting and Multiplexed Analog Components (MAC). Signal reformatting, often called sync suppression, is an approach in which video sync pulses are removed and the video signal is inverted. MAC uses a non–standard format to encode audio, luminance, and color to prevent unwanted interception of video signals. Video scrambling can be either analog or digital, but both are based on a methodology which alters the format of a video signal to obscure information.

DIGITAL VIDEO SCRAMBLING

Digital scrambling tends to be more secure than analog methods. Classified information gathered by unmanned systems which is deemed critical to the intelligence community would require more secure scrambling techniques such as those provided by a digital bit by bit encryption. A digital bit by bit encryption uses pseudo random sequences to alter the digitized audio and video signals. Digital video encryption has become more practical with the advent of image compression algorithms. Digital encryption of video images offers a more secure method for protecting sensitive information, but extracts a cost in terms of expense and computational intensity. Encrypting video information after sampling and digitizing would necessitate transmission of approximately 90 MBPS, which would require compression to be used in real time.

DATA ENCRYPTION OVERVIEW

The development of secret coding and protection of valuable information is often referred to as cryptology. Cryptography is the mathematical transformations of algorithms which along with a key are used to encrypt or encode plaintext into unintelligible data, which is often referred to as ciphertext. Encryption schemes usually can be broken into one of two categories: block encryption and data–stream encryption. Block encryption groups the plaintext into blocks of a fixed size which are independently encrypted, while data–stream ciphers have no fixed block size and the data is treated as a stream of bits. The process of attacking this encoded data to recover the plaintext and compromise this sensitive information is called cryptanalysis. There are several methods of attack employed by the cryptanalyst to try to recover the secret key using his knowledge of the plaintext and ciphertext.

ENCRYPTION ALGORITHMS

Cryptographic transforms or algorithms are the focus of much research and are considered vital to national security. They tend to be tightly controlled and are often classified. Encryption algorithms are generally based on substitution/permutation schemes or obscure number theory problems which have been traditionally proven extremely difficult to solve. Encryption algorithms are under constant attack from advances in mathematics and the increasing power of high speed computing. To ensure security, the encryption algorithms must be complex and defy an analytical solution. They must also require the attacker to consume a prohibitive amount of resources (time and money) to launch a successful attack. The term work factor is often used to access the strength of an encryption scheme. The work factor is the amount of resources needed to break an encryption algorithm.

SYMMETRICAL ENCRYPTION

Traditional encryption systems are known as symmetrical or private key encryption. This type of encryption uses the same key for both encryption and decryption (Fig. 2). This method of encryption requires that the key be kept secret, making key management and distribution paramount. The most widely known of these symmetrical encryption schemes is the Data Encryption Standard (DES), developed by IBM under the guidance of the National Security Agency (NSA). DES has been acknowledged as a world–wide standard and has been widely used by the government, banks, and financial agencies for over 15 years. The DES is a block cipher and encrypts data in blocks of 64–bits, using a 56–bit key. DES is based on a substitution–per–permutation model, where the key is mixed with the plaintext and substitutions are made to change each block to transform the plaintext into ciphertext (Fig. 3). To prevent the cryptanalyist from using statistical analysis of the frequency of occurrence by individual or combinations of characters, transformations like DES use the concepts of contusion and diffusion. Confusion attempts to invoke substitutions that make the relationship between the ciphertext and key as complicated as possible. Diffusion is used to average out the statistical variances between characters and groups of characters. These transformations are implemented through the use of substitution–boxes (s–boxes) and permutation–boxes (p–boxes). The use of s–boxes and p–boxes alone would not frustrate an experienced cryptanalysis, but the combination of s–boxes and p–boxes can provide a formidable crypto–system. Many experts believe that the 56–bit key length, while effective against 1970's technology, needs to be increased to 128–bits to improve security and make the algorithm effective against the advances in high speed computing. The establishment of an encryption standard may not be wise since it makes a tempting target for adversaries to focus their resources. Breaking an encryption system used by a large number of sources for both civilian and military information would be a major coup to a potential adversary. Symmetrical encryption systems like DES are widely known and have been studied for many years which means that the security of the system depends on choosing a strong key and keeping it secret.

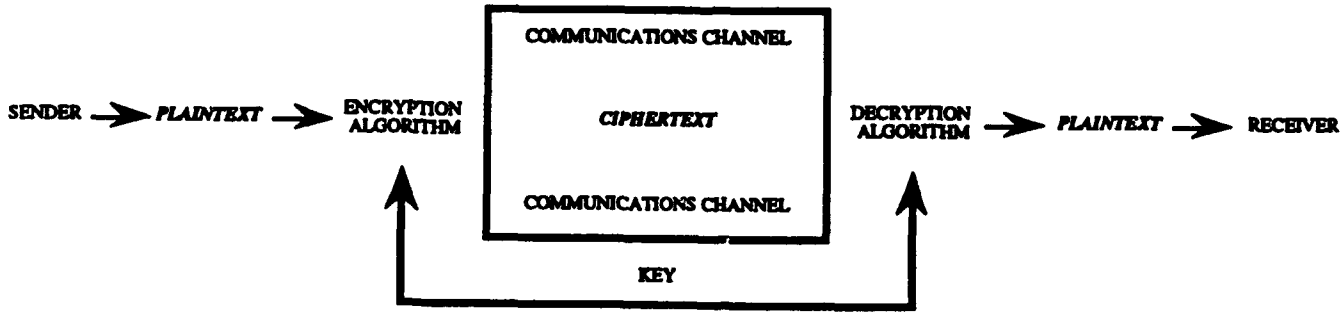


Figure 2. Symmetrical Encryption

DATA ENCRYPTION STANDARD (DES)

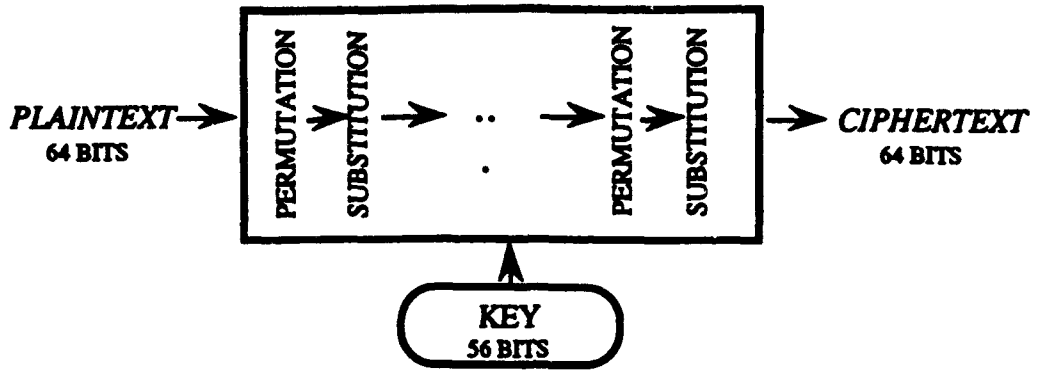


Figure 3. DES Substitution–Permutation

IMPORTANCE OF CHOOSING A KEY

Increasing the key length of a symmetrical encryption system like DES is one way to dramatically decrease your vulnerability to a brute force attack. A brute force attack is when every possible combination of keys is tried to break the secret code. The importance of choosing a secure key and the management of keys can not be overemphasized. In many cases, something is known about the encryption algorithm, so much of encryption is concerned with keeping the key safe rather than the encryption algorithms. Keys should be truly random and not simply chosen from words in the dictionary. There are less than one million words in the dictionary, and the use of a key from such a small subset of possible keys would make the cryptanalysis job easy. Rumor has it that many drug dealers have found this out the hard way and are living rent free in prison, courtesy of the federal government. Keys should be random and non repeatable. One should be careful of using digital computers for choosing keys since the pseudo random numbers it generates tend to be repeatable and not suitable for selecting a key.

ASYMMETRICAL ENCRYPTION

No discussion of encryption would be complete without mentioning asymmetrical encryption, which is commonly called Public Key Cryptography (PKC). PKC is based on the notion of using a pair of keys, one public and one private (Fig. 4). Public keys may be known to all and even published in a book for other users. The message is encoded with the private key and decoded with the public key or vice versa. This concept centers on the fact that even knowing the public key, it is not feasible to determine the private key. PKC algorithms are largely based on obscure number theory problems that have proven difficult to solve even with sophisticated algorithms and large amounts of computer power. At the heart of PKC systems are trapdoor one–way functions which are easy to compute one–way but are computationally infeasible to reverse. A simple example may help illustrate. For the function below the value of Y is easy to find given X, but the value of X given Y would be more computationally intensive.

$$Y = X^5 + 3X^4 + 75X^3 + 350X^2 + 423$$

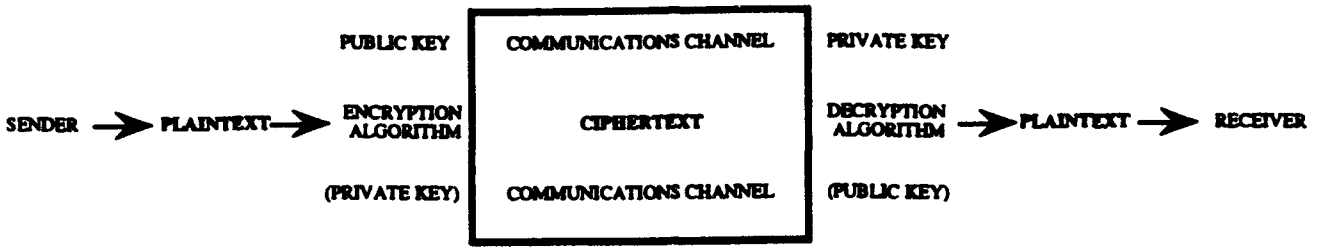


Figure 4. Asymmetrical Encryption

Many of these trapdoor one–way functions are based on problems whose origins can be traced to number theory. Some of the better known and more widely used algorithms are based on prime factorization, the theory of elliptical curves and the discrete logarithm function. PKC allows not only secrecy and integrity of information but message authentication as well. This example may help to illustrate. If person B uses person A's public key to encrypt a message then only person A can decrypt this message with his private key. If person A encrypts a message with his private key, then anyone using person A's public key can decrypt the message, and be sure that person A sent the message (message authentication). PKC is relatively new and first became public in the 1970's. The most widely know PKC algorithm is the RSA. RSA is based on the concept that it is very difficult to factor large prime numbers (at least 100 digits). Both the public and private key are derived from very large prime numbers and attempting to determine one key from another is tantamount to factoring the product of these two prime numbers.

TRADEOFFS

There are many things to consider in choosing an information security technology. These considerations include the level of security required, technical sophistication of potential adversaries, the amount of information to be protected, the time sensitivity of the information (length of time this information has value), and the computational intensity required to implement the system. It is important to focus on the level of security of the information being secured. Traditional analog scrambling is often a cheap and easy method to secure information but does not offer a high degree of security. Even compression schemes could help disguise information from the casual eavesdropper, but more sophisticated techniques would be needed to fool a serious cryptanalyist. Some classified information has value for only a short length of time and therefore if a brute force attack could reveal this information in two weeks, it may be of no value to a potential adversary. Other information needs to be kept secret for decades and only the most secure algorithm should be used to protect this information. The amount of information needed to be protected and the computational intensity of the algorithm must be weighed before choosing a crypto–system. Public key encryption tends to be computationally intensive and requires longer processing times and is not recommended for bulk encryption. Public key encryption may be most effective for key management and distribution. Traditional private encryption such as DES with an extended key length is probably still the most feasible method for securing electronic intelligence gathered by unmanned systems.

CONCLUSIONS

Unmanned systems are involved in the collection of electronic intelligence and information gathered by these systems are critical to the overall decision making process. Information collected by these systems can be of a sensitive nature and steps to ensure the integrity and secrecy of this information should be examined. This report briefly discussed the mission of unmanned systems, the importance of information security, video scrambling, symmetrical and asymmetrical encryption. Finally, a brief discussion of factors that should be considered when choosing a method of safeguarding the integrity and secrecy of the information were examined.

REFERENCES

1. Beker, H. and Piper F., Cipher Systems, John Wiley & Sons Inc., New York, 1982.

2. Boyd, C., "Modern Data Encryption", Electronics & Communications Engineering Journal, October 1993.

3. Cambell, Carl M., "Design & Specification of Cryptographic Capabilities," IEEE Communications Society Magazine, November 1978, Vol. 16, No 6, pp. 15–19.

4. Dror, Asael, "Secret Codes", BYTE Magazine, June 1989.

5. Gleason, Thomas J., "Data Link Tradeoffs for Unmanned Aerial Vehicles," Gleason Research Associates Incorporated, Columbia, MD 21044.

6. National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standard, Publication no. 46, Jan 1977.

7. Riek, Justas, "Applications of Public Key Cryptography to Computer/Communications Security," Data Systems Division, Grumman Corporation, 1987.

ACRONYMS

DES	Data Encryption Standard
MAC	Multiplexed Analog Component
MBPS	Megabits per Second (1 million bits per second)
NSA	National Security Agency
PKC	Public Key Cryptography

BIOGRAPHY

John R. Coward works as an electronics engineer at the U. S. Army Missile Command in Huntsville, Alabama. He has worked on both unmanned aerial and ground vehicles. His primary interest include computer and information security, encryption, worms/viruses, and TEMPEST.

INITIAL DISTRIBUTION LIST

	Copies
AMSMI–RD	1
AMSMI–RD–AC	1
AMSMI–RD–AC–AD	1
AMSMI–RD–AC–AD, S. Young	1
AMSMI–RD–AC–CA	1
AMSMI–RD–AS	1
AMSMI–RD–AS–MM	1
AMSMI–RD–AS–PM	1
AMSMI–RD–BA	1
AMSMI–RD–BA–CSI	1
AMSMI–RD–BA–TU	1
AMSMI–RD–CS–R	3
AMSMI–RD–CS–T	1
AMSMI–RD–GC	1
AMSMI–RD–GC–S	1
AMSMI–RD–SE	1
AMSMI–RD–SE–EA	1
AMSMI–RD–SE–ES	1
AMSMI–RD–SE–PE, A. Roberts	1
AMSMI–RD–SI	1
AMSMI–RD–SI, D. Trenkle	1
AMSMI–RD–SS	1
AMSMI–RD–SS–SP, K. Flynn	1
AMSMI–RD–WS	1
AMSMI–RD–WS–LS, D. Jordan	1